Risk is Risk, Right?

PM Challenge 2007

Joshua Krage
NASA Goddard Space Flight Center
Greenbelt, MD

Agenda

- Review of risk assessment processes
  - Equations
  - Likelihood
  - Impact
  - Human impact
- Review of risk dialects
  - Management of programs and projects
  - Engineering efforts
  - Security concerns
- Final comparisons and recommendations

What is Risk?

- We deal with risk every day
  - Each of us has an instinctual understanding of how to discern “day-to-day” risk, and avoid too much of it
- But… do we:
  - mean the same thing?
  - make the same assessments?
  - manage the same risk?
- Definition:

  (noun)

  1: a situation involving exposure to danger.
  2: the possibility that something unpleasant will happen.
  3: a person or thing causing a risk or regarded in relation to risk
  (Compact Oxford English Dictionary, www.askoxford.com)

Many Risk Disciplines

- Many disciplines use risk and risk assessment language
  - Psychology (decision theory)
  - Statistics
  - Financial institutions
  - Scenario analysis

- While fascinating, these are (mostly) out of scope for today's discussion

- Today we focus on management, engineering, and security risk

Risk Equations

The various risk disciplines distill a complex process into a easy-to-remember equation, with slight variances in approach and language.

Source	Risk Equation
ISO17666:2003	Likelihood x Severity = Risk
NIST SP800-30	Likelihood x Impact = Risk
NASA NPR8000.4	Likelihood x Consequences = Risk
Probabilistic Risk Assessment	Probability(of Event) x Consequence = Risk
Security Risk	P(threat) x P(vulnerability) x Impact = Risk P(threat) x P(vulnerability) x Cost = Risk
Engineering & Safety Risk	P(accident) x LossesPerAccident = Risk

The commonality in these equations supports thinking of risk assessment as a uniform process.

Picking Apart Likelihood

- Likelihood is usually measured in terms of probability
  - The probability a particular outcome will be achieved
    - Ex. 98% chance the audience understands this
  - Generally considered an objective measurement
  - Can be derived mathematically (through proofs) or experientially
- Challenges:
  - Basic probability assumes all outcomes are equal
    - Ex. Flipping a coin yields either heads or tails
  - True probability allows for some uncertainty
    - Ex. It is statistically improbable for the coin to land on its edge; or even not to land
  - Requires data from outcomes of similar situations
    - The longer the baseline, the better the data
  - Experiential data is generally time-bound
    - Ex. Flood of the century
  - If other techniques are not sufficient, then one is left with estimates and judgement calls

Picking Apart Threats & Vulnerabilities

- Some risk assessment techniques (e.g. security) split likelihood into threats and vulnerabilities
  - Vulnerability indicates a weakness in a specific area or function, which if exploited will cause impact
  - Threat indicates the source or actor which can exploit the vulnerability
  - If neither a threat nor a vulnerability exist, then no risk
  - Usually have the most control over vulnerabilities, not threats

- Examples of threats (exploits) and vulnerabilities:
  - Sick birds can infect healthy but non-immunized birds
  - Wind can generate un-dampened oscillations in an overly fluid bridge
  - Continuing resolutions will delay new work in the US Federal Government
  - A cracker will break into a misconfigured database to steal credit card numbers

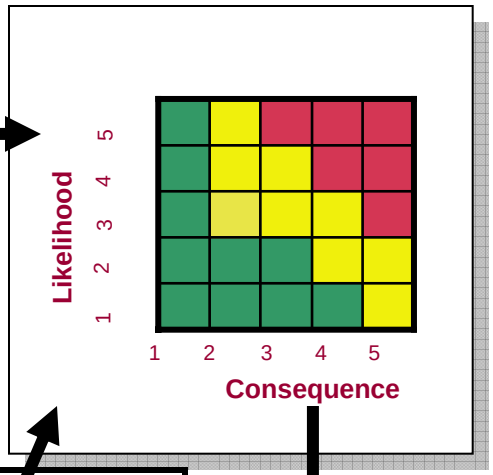
Picking Apart Impact

- Impact has many measuring systems
  - Cost is the most common objective measurement
  - Many impacts are intangible
    - Ex. Reputation/image, politics, copying intellectual property, etc.
    - These are measured subjectively: mild, moderate, severe, catastrophic
  - Typically rated in terms of Confidentiality, Integrity, and Availability

- Challenges:
  - Accurate cost impact assessments require a sufficient level of cost data
  - Intangible impacts depend on a subjective assessment
    - Frequently inconsistent among reviewers
    - Breaches of confidentiality and integrity are typically the most challenging to assess

Exhibit: 5x5 Risk Matrix in Four Areas

Likelihood Bins	Safety (Likelihood of safety event occurrences)	Technical (Estimated Likelihood of not meeting mission technical performance requirements)	Cost/Schedule (Estimated Likelihood of not meeting allocated Cost/Schedule requirement or margin)
5 Very High	($P_S > 10^{-1}$)	($P_T > 50\%$)	($P_{CS} > 75\%$)
4 High	($10^{-2} < P_S < 10^{-1}$)	($25\% < P_T < 50\%$)	($50\% < P_{CS} \leq 75\%$)
3 Moderate	($10^{-3} < P_S < 10^{-2}$)	($15\% < P_T < 25\%$)	($25\% < P_{CS} \leq 50\%$)
2 Low	($10^{-6} < P_S < 10^{-3}$)	($2\% < P_T < 15\%$)	($10\% < P_{CS} \leq 25\%$)
1 Very Low	($P_S < 10^{-6}$)	($0.1\% < P_T < 2\%$)	($P_{CS} \leq 10\%$)



Consequence Categories

Risk Type	1 Very Low	2 Low	3 Moderate	4 High	5 Very High
Safety	Negligible or No impact.	Could cause the need for only minor first aid treatment .	May cause minor injury or occupational illness or minor property damage.	May cause severe injury or occupational illness or major property damage.	May cause death or permanently disabling injury or destruction of property.
Technical	No impact to full mission success criteria	Minor impact to full mission success criteria	Moderate impact to full mission success criteria. Minimum mission success criteria is achievable with margin	Major impact to full mission success criteria. Minimum mission success criteria is achievable	Minimum mission success criteria is not achievable
Schedule	Negligible or no schedule impact	Minor impact to schedule milestones; accommodates within reserves; no impact to critical path	Impact to schedule milestones; accommodates within reserves; moderate impact to critical path	Major impact to schedule milestones; major impact to critical path	Cannot meet schedule and program milestones
Cost	<2% increase over allocated and negligible impact on reserve	Between 2% and 5% increase over allocated and can handle with reserve	Between 5% and 7% increase over allocated and can not handle with reserve	Between 7% and 10% increase over allocated, and/or exceeds proper reserves	>10% increase over allocated, and/or can't handle with reserves

HIGH RISKS

MODERATE RISKS

LOW RISKS

Human Factors

- The brain does funny things with risk
  - Humans have a tendency to subconsciously ignore or downplay the “edge” risks (implicit acceptance)
    - Extreme impact: don’t think about it
    - Low impact: not a big deal
    - High likelihood: what can you do?
    - Low likelihood: will never happen
    - Low occurrence rate with low impact: not a big deal
  - Subjective assessments allow the brain to insert its bias and can skew results

- Mitigations:
  - Use objective assessments as a baseline where possible
  - Use peer reviews with common definitions to validate results

Reviewing the Bidding

- Many disciplines, but a common terminology
  - Risk = Likelihood x Impact (Threat & Vulnerability)
- Likelihood
  - Typically presented in mathematical probability terms
  - Frequently includes some estimation or judgement call
- Impact
  - Very subjective
  - Varying units of measure
- If not controlled, humans can skew assessments
- Varied results are common, despite common language and approach

Risk Management

- Four classic strategies to handle risk:
  - Accept
    - Do nothing
  - Eliminate
    - Force likelihood (or threat or vulnerability) OR impact to zero
  - Mitigate
    - Do something to limit the likelihood or reduce the impact, but not completely
  - Transfer
    - Assign someone else the acceptance of the risk, usually through insurance
- Risk ignorance is equivalent to implicit risk acceptance

Management Risk

- Project risk focuses primarily on schedule and resources (people, equipment, locations, money)
  - Good project managers consider the other areas as well, but the expectations set for the project manager are based in management risk
  - New issues (nascent risks) are tracked with increasing measurements
  - Lack of change or action is equal to lack of changing risk (controlled variables)
  - Risks tend to be eliminated or accepted, sometimes mitigated, rarely transferred
  - Politics plays a frequent (undocumented) role
- Managerial decisions define the overall project's risk management strategy
  - Drives all other risk areas
  - Can override technical concerns (appropriately)
  - Generally provides the most flexibility to the project

Engineering Risk

- Engineering risk has its base in applied technology
  - Pushing the envelope of technology is a common goal of engineering risk
  - Given enough freedom, engineers can address most challenges successfully
  - Engineering is a critical component to mission success -- it cannot be ignored
  - Impact is usually that something breaks or progress down a path is stopped
  - Extensive materials and methods baselines are available
    - Aggressive testing can help develop or extend the baseline, even into conditions outside of “normal”
    - Partial matches to existing baselines can be extrapolated with low uncertainty
  - Not all risks can be mitigated; some have to be accepted
    - Ex. Comet hits deep space probe
  - Risks to others (safety) exist, but can usually be quantified
  - Risks are frequently mitigated or eliminated, sometimes accepted, and rarely transferred

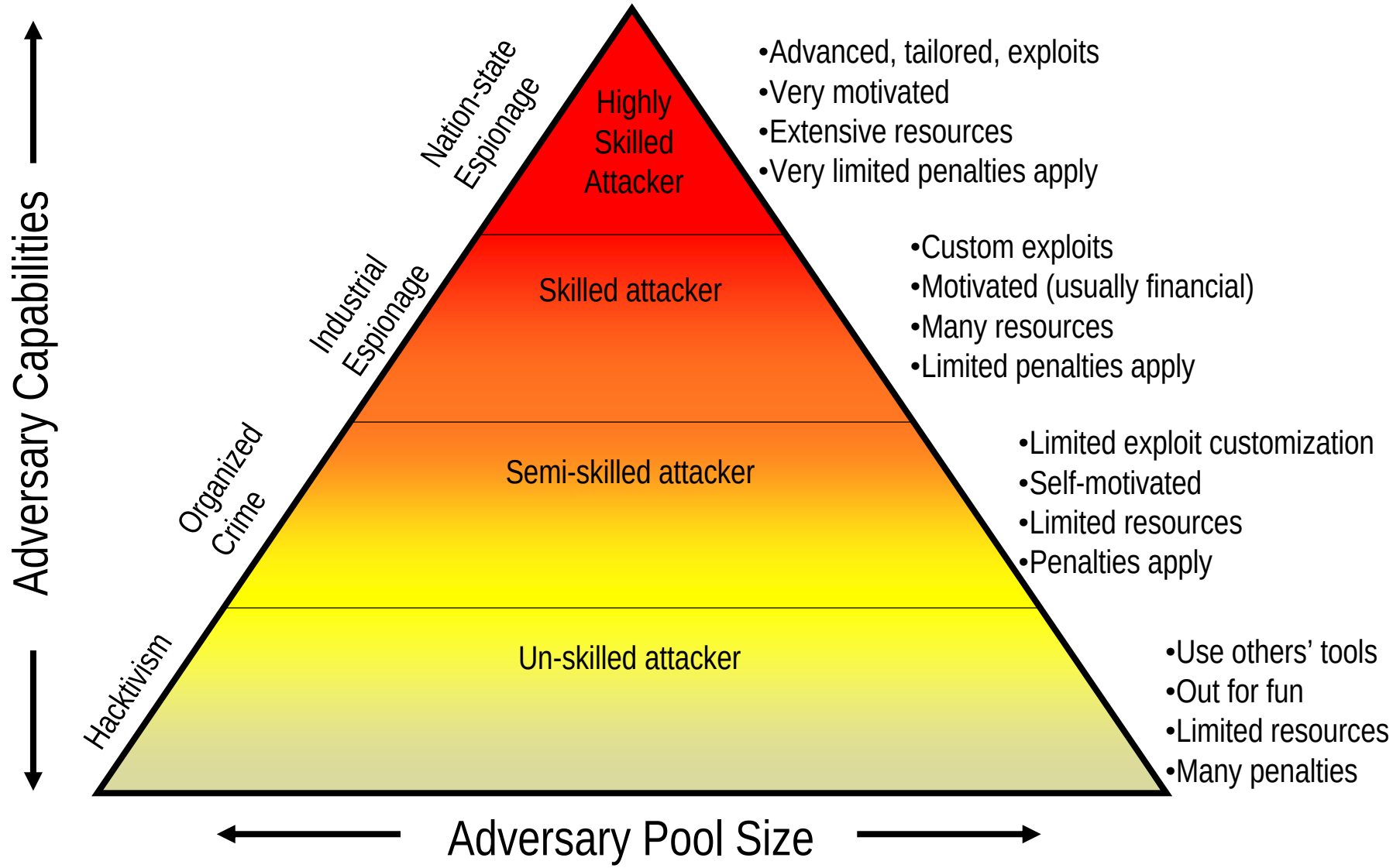
Security Risk

- Security risks (both physical and information) are generally about people and only sometimes about technology
  - Security protects and enables the project (or it is supposed to, anyway)
  - Security should be considered across the project, but is frequently underutilized
  - Good security staff are creatively paranoid; they expect the unexpected
  - Mitigations or eliminations are almost always possible, given sufficient resources
    - Various points of diminishing returns, and mitigation is rarely 100% guaranteed
  - "New" vulnerabilities are constantly identified
    - Generally already exist; we were just unaware of their existence (risk ignorance)
  - Risk to others is frequently challenging to quantify
    - Ex. Your home computer being used to attack others
  - Many security guides focus on implementing appropriate controls, not measuring or tracking the process output (i.e. tracking how the control is effective)
  - Risks are commonly mitigated, and sometimes accepted, eliminated, or transferred

Adaptive Adversaries

- The single largest difference between security risk and others is the concept of the "intelligent, adaptive adversary"
  - Project management has many things to deal with, but sabotage is not common
  - Engineers plan to overcome natural and incidental human-triggered risks
  - Security staff focus on adversaries and situations where both deliberate and accidental actions are important
  - Adversaries continually adapt and evolve, unlike most natural threats
  - The adversary is the perfect example of an uncontrolled variable
    - It is rare to be able to limit the adversary's threat source
  - The attacking adversary can choose which vulnerability to attack to what degree while the defender must address all possible vulnerabilities
  - Quantifying the adversary is very subjective
  - The types of adversary vary widely

Adversary Pyramid



Final Comparisons

- Risk language is consistent, with common approaches
  - Various dialects of the same language, with custom terminology and assumptions
  - The mechanics are simple to understand, if complex to implement
  - Results can be varied across the dialects
  - Subjective elements can be hidden by the terminology
- Commonalities between dialects exist:
  - Management and security risk is mostly about people and communications, and have the most intangibles to assess in impact
  - Engineering and security risk have the least control over external variables, and are always identifying previously-unknown latent issues
  - Management and engineering risk can depend on long baselines of prior experience
- Some uniqueness exists:
  - Management risk includes politics
  - Engineering risk is the most straight-forward to quantify
  - Security risk includes the adaptive adversary

Final Recommendations

- Set the risk management approach and tone early
  - Ensure risk management is utilized throughout the project lifecycle
  - Engage the subject matter experts early and often
  - Identify the risk management approach(es) to be used for each dialect and ensure all staff are familiar with the approach
  - Be aware of the dialect differences in risk discussions
  - Communicate continuously about risk issues across the project; cross-breed awareness between the subject matter teams
  - Identify the subjective elements of the risk assessment and repeatedly re-evaluate

- As with most project problem solutions, communications is a key element to managing risk

Questions?

- Any questions?

- Contact information:
  - Joshua Krage
    Joshua.Krage@nasa.gov

Backup Slides

Action Learning

- Need three audience volunteers
  - One project manager/engineer
  - Two operatives, not assigned to the project
- Project: Toss
  - Mission success criteria
    - Using the provided components (balls/beanbags), get as many as possible into the target receptacle within the time provided (the schedule)
  - Constraints
    - Resources (staff and components) are limited to those specifically provided
    - Project staff may not approach within the minimum distance indicated until all components have been used
    - Others as indicated
- Operatives receive special instructions individually

References

- ISO17666:2003: Space Systems -- Risk Management
  http://www.iso.org/ (available for purchase)

- NIST SP800-30: Risk Management Guide for Information Technology Systems
  http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

- NASA NPR8705.5: Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
  http://nodis.hq.nasa.gov/ (download site)

- NASA NPR8000.4: Risk Management Procedural Requirements
  https://nodis.hq.nasa.gov/ (download site)

Additional Reading

- European Network and Information Security Agency (ENISA): Risk Management: Implementation Principles and Inventories for Risk Management/Risk Assessment Methods and Tools
  http://www.enisa.europa.eu/rmra/files/D1_Inventory_of_Methods_Risk_Management_Final.pdf

- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  http://www.cert.org/octave/

- Information Security Management Maturity Model (ISM3)
  http://www.ism3.com/ Process oriented information security management